Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered t o be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
3Com Network Supervisor 5.0.2, Network	An input validation/ directory traversal vulnerability has been reported in Network Supervisor that could let remote malicious users disclose files.	3Com Network Supervisor File Disclosure	Medium	Secunia, Advisory: SA16639, September 2,

Director 1.0, 2.0	Vendor patch available: Network Director 1.0 (up to and including SP1): http://support.3com.com/software/3Com_network_director_v1_0_sp0_1_cu1.exe Network Director 1.0 (SP2 and SP3): http://support.3com.com/software/3Com_network_director_v1_0_sp2_3_cu1.exe Network Director 2.0: http://support.3com.com/software/3com_network_director_v2_0_cu1.exe Network Supervisor 5.1: http://support.3com.com/software/3com_network_supervisor_v5_1_cu1.exe There is no exploit code required.	CAN-2005-2020		2005
Altools ALZip 5.51, 5.52, 6.03, 6.1beta, 6.11	A buffer overflow vulnerability has been reported in ALZip (ACE archives) that could let a malicious users obtains unauthorized system control. Upgrade to version 6.1 : http://www.altools.net/Portals/0/ALZip.exe There is no exploit code required.	ALZip Unauthorized System Control CAN-2005-2856	Medium	Secunia Advisory: SA16479, September 7, 2005
AttachmateWRQ Reflection for Secure IT Windows Server 6.0	Multiple vulnerabilities have been reported in Reflection for Secure IT that could let malicious users disclose information or obtain unauthorized access. Vendor workaround available: http://support.wrq.com/techdocs/1867.html There is no exploit code required.	Reflection for Secure IT Multiple Vulnerabilities CAN-2005-2770 CAN-2005-2771	Medium	Security Tracker Alert ID: 1014835, September 1, 2005 US-CERT VU#758054 US-CERT VU#902110
Dameware Dameware prior to 4.9.0	A vulnerability has been reported in Dameware that could let remote malicious users execute arbitrary code. Upgrade to version 4.9.0: http://www.dameware.com/download An exploit script has been published.	DameWare Arbitrary Code Execution CAN-2005-2842	High	Security Focus, 14707, August 31, 2005 US-CERT VU#170905
Free SMTP Free SMTP Server 2.2	A vulnerability has been reported in Free SMTP Server that could let remote malicious users create an open mail relay. No workaround or patch available at time of publishing. An exploit script has been published.	Free SMTP Server As Open Relay CAN-2005-2857	Medium	Secunia Advisory: SA16698, September 5, 2005
Indiatimes Messenger Indiatimes Messenger6.0	A buffer overflow vulnerability has been reported in Indiatimes Messenger that could let malicious users cause a Denial of Service. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Indiatimes Messenger Denial of Service CAN-2005-2844	Low	Security Tracker Alert ID: 1014842, September 2, 2005
Microsoft Windows 2000 SP3 and SP4 Windows XP SP1 and SP2 Windows XP 64-Bit Edition SP1 and 2003 (Itanium) Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows 98, 98 SE, and ME	Multiple vulnerabilities have been reported that include errors in the font, Kernel, Object Management Vulnerability and CSRSS. These are due to input validation and buffer overflow errors. A malicious user could deny service or obtain escalated privileges. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-018.mspx **An exploit has been published.**	Microsoft Windows Kernel Elevation of Privilege and Denial of Service Vulnerabilities CAN-2005-0060 CAN-2005-0061 CAN-2005-0550 CAN-2005-0551	Medium	Microsoft Security Bulletin MS05-018, April 12, 2005 US-CERT VU#259197 US-CERT VU#775933 US-CERT VU#943749 US-CERT VU#650181 **Security Focus, 13115, September 6, 2005**

Rediff Bol Rediff Bol 7.0	A vulnerability has been reported in Rediff India Abroad that could let remote malicious users disclose the Window's address book. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Rediff Bol Window's Address Book Disclosure CAN-2005-2858	Medium	Secunia, Advisory: SA16685, September 5, 2005
Savant Savant Web Server 3.1	A vulnerability has been reported in Savant Web Server that could let local malicious users disclose other user information. No workaround or patch available at time of publishing. There is no exploit code required.	Savant Web Server User Information Disclosure CAN-2005-2859	Medium	Secunia Advisory: SA16666, September 6, 2005
SlimFTPd 3.17	A vulnerability has been reported in SlimFTPd (USER and PASS commands) that could let a remote malicious users cause a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	SlimFTPd Denial of Service CAN-2005-2850	Low	Security Tracker, Alert ID: 1014831 , September 1, 005
Symantec Symantec Anti Virus Corporate Edition (LiveUpdate 2.7)	A vulnerability has been reported in Symantec Anti Virus (internal LiveUpdate feature) that could let local malicious users disclose password information. Upgrade to newest version of LiveUpdate: http://www.symantec.com/techsupp/files/lu/lu.html These is no exploit code required.	Symantec Anti Virus Password Disclosure CAN-2005-2766	Medium	Security Tracker Alert ID: 1014834, September 1, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Adobe Adobe Version Cue 1.0.1, 1.0	A vulnerability has been reported due to insecure file permissions on internal Version Cue application files, which could let a malicious user obtain elevated privileges. Patches available at: http://www.adobe.com/support/downloads/detail.jsp?ftpID=2985 **Exploit scripts have been published.**	Adobe Version Cue for Mac OS X Elevated Privileges CAN-2005-1842 CAN-2005-1843	Medium	Security Focus, Bugtraq ID: 14638, August 23, 2005 **Security Focus, Bugtraq ID: 14638, August 31, 2005**
Apache Software Foundation Apache 2.0.x	A vulnerability has been reported in 'modules/ssl/ssl_engine_kernel.c' because the 'ssl_hook_Access()' function does not properly enforce the 'SSLVerifyClient require' directive in a per-location context if a virtual host is configured with the 'SSLVerifyCLient optional' directive, which could let a remote malicious user bypass security policies. Patch available at: http://svn.apache.org/viewcvs?rev=264800&view=rev OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html Ubuntu:	Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass CAN-2005-2700	Medium	Security Tracker Alert ID: 1014833, September 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.017, September 3, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005

	http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ There is no exploit code required.			
CVS CVS 1.12.7-1.12.12, 1.12.5, 1.12.2 , 1.12.1, 1.11.19, 1.11.17	A vulnerability has been reported in the 'cvsbug.in' script due to the insecure creation of temporary files, which could let a malicious user cause data loss or a Denial of Service. **Misclassified as multiple operating systems.** Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:20/cvsbug.patch** **SGI:** **ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** There is no exploit code required.	CVS 'Cvsbug.In' Script Insecure Temporary File Creation CAN-2005-2693	Low	Fedora Update Notifications FEDORA-2005-790 & 791, August 23, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0045, August 26, 2005** **RedHat Security Advisory, RHSA-2005:756-3, September 6, 2005** **SGI Security Advisory, 20050901-01-U, September 7, 2005** **FreeBSD Security Advisory, FreeBSD-SA-05:20, September 7, 2005**
frox frox 0.7.18	A vulnerability has been reported which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Frox Arbitrary Configuration File Access CAN-2005-2807	Medium	Security Focus Bugtraq ID: 14711, September 1, 2005
Gentoo net-analyzer/net-snmp 5.2.1 .2, 5.2.1 -r1	A vulnerability has been reported because a malicious user with portage group privileges can create a shared object that will be loaded by the Net-SNMP Perl modules, which could lead to elevated privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200509-05.xml There is no exploit code required.	Gentoo Net-SNMP Elevated Privileges CAN-2005-2811	Medium	Gentoo Linux Security Advisory, GLSA 200509-05, September 6, 2005
GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a file with the '-N' flag, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/	GNU GZip Directory Traversal CAN-2005-1228	Medium	Bugtraq, 396397, April 20, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Security Focus,13290, May 11, 2005

	glsa/glsa-200505-05.xml IPCop: http://ipcop.org/modules.php?op=modload&name=Downloads&file=index&req=viewdownload&cid=3&orderby=dateD Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch OpenPKG: http://www.openpkg.org/security/OpenPKG-SA-2005.009-openpkg.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/g/gzip Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101816-1 **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-172.pdf** Proof of Concept exploit has been published.		Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.009, June 10, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Conectiva Linux Announce-ment, CLSA-2005:974, July 6, 2005 Debian Security Advisory DSA 752-1, July 11, 2005 Sun(sm) Alert Notification Sun Alert ID: 101816, July 20, 2005 **Avaya Security Advisory, ASA-2005-172, August 29, 2005**

GNU gzip 1.2.4, 1.3.3	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-05.xml Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:11/gzip.patch RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Debian: http://security.debian.org/pool/updates/main/g/gzip/gzip Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101816-1 **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-172.pdf** There is no exploit code required.	GNU GZip File Permission Modification CAN-2005-0988	Medium	Security Focus, 12996, April 5, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:11, June 9, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Conectiva Linux Announce-ment, CLSA-2005:974, July 6, 2005 Debian Security Advisory DSA 752-1, July 11, 2005 Sun(sm) Alert Notification Sun Alert ID: 101816, July 20, 2005 **Avaya Security Advisory, ASA-2005-172, August 29, 2005**
GNU wget 1.9.1	A vulnerability exists which could permit a remote malicious user to create or overwrite files on the target user's system. Wget does not properly validate user-supplied input. A remote user can bypass the filtering mechanism if DNS can be modified so that '..' resolves to an IP address. A specially crafted HTTP response can include control characters to overwrite portions of the terminal window. SUSE: ftp://ftp.SUSE.com/pub/SUSE Mandriva: http://www.mandriva.com/security/advisories Trustix:	GNU wget File Creation & Overwrite CAN-2004-1487 CAN-2004-1488	Medium	Security Tracker Alert ID: 1012472, December 10, 2004 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 SUSE Security Summary Report, SUSE-SR:2005:006, February 25, 2005 SUSE Security Summary Report, SUSE-SR:2005:011, April 15, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:098, June 9, 2005 Trustix Secure Linux

	http://http.trustix.org/pub/trustix/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/w/wget/** A Proof of Concept exploit script has been published.			Security Advisory, TLSA-2005-0028, June 13, 2005 Turbolinux Security Advisory, TLSA-2005-66, June 15, 2005 Ubuntu Security Notice, USN-145-1, June 28, 2005 **Ubuntu Security Notice, USN-145-2, September 06, 2005**
GNU zgrep 1.2.4	A vulnerability has been reported in 'zgrep.in' due to insufficient validation of user-supplied arguments, which could let a remote malicious user execute arbitrary commands. A patch for 'zgrep.in' is available in the following bug report: http://bugs.gentoo.org/show_bug.cgi?id=90626 Mandriva: http://www.mandriva.com/security/advisories TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-357.html RedHat: http://rhn.redhat.com/errata/RHSA-2005-474.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ SGI: http://www.sgi.com/support/security/ F5: http://tech.f5.com/home/bigip/solutions/advisories/sol4532.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gzip/ Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-172.pdf** There is no exploit code required.	Gzip Zgrep Arbitrary Command Execution CAN-2005-0758	High	Security Tracker Alert, 1013928, May 10, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005 Turbolinux Security Advisory, TLSA-2005-59, June 1, 2005 RedHat Security Advisory, RHSA-2005:357-19, June 13, 2005 RedHat Security Advisory, RHSA-2005:474-15, June 16, 2005 SGI Security Advisory, 20050603-01-U, June 23, 2005 Fedora Update Notification, FEDORA-2005-471, June 27, 2005 SGI Security Advisory, 20050605-01-U, July 12, 2005 Secunia Advisory: SA16159, July 21, 2005 Ubuntu Security Notice, USN-158-1, August 01, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 **Avaya Security Advisory, ASA-2005-172, August 29, 2005**

Hewlett-Packard HP-UX B.11.00, B.11.11, B.11.22, B.11.23; only if converted to trusted systems	A vulnerability has been reported that could let a remote malicious user access the system. HP-UX systems that have been converted to trusted systems contain an unspecified vulnerability that allows a remote user to gain unauthorized access to the target system. The vendor has issued the following fixes, available at: http://itrc.hp.com For HP-UX B.11.00 - PHCO_29249 and PHNE_17030 For HP-UX B.11.11 - PHCO_33215 For HP-UX B.11.23 - PHCO_32926 For HP-UX B.11.22, action: disable remshd (OS-Core.CORE2-SHLIBS) and avoid the telnet -t option. **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-169.pdf** Currently we are not aware of any exploits for this vulnerability.	HP-UX Trusted Systems Grant Access to Remote Users CAN-2005-1771	Medium	HP Security Bulletin, HPSBUX01165 REVISION: 0, SSRT5899 rev.0, May 25, 2005 **Avaya Security Advisory, ASA-2005-169, August 29, 200**
Inter7 SqWebMail 5.0.4	A vulnerability has been reported because the '<script>' tag can be used in HTML comments, which could let a remote malicious user execute arbitrary code when malicious email is viewed. Patch available at: http://www.courier-mta.org/beta/sqwebmail/ There is no exploit code required; however, a Proof of Concept exploit has been published.	SqWebMail HTML Email Script Tag Script Injection CAN-2005-2820	Medium	Secunia Advisory: SA16704, September 6, 2005
Inter7 SqWebMail 5.0.4, 5.0 .1, 5.0.0, 4.0.5 -4.0.7, 4.0.4.20040524, 3.6.1, 3.6 .0, 3.5.0-3.5.3 , 3.4.1	A vulnerability has been reported due to insufficient sanitization of HTML emails, which could let a remote malicious user execute arbitrary HTML and script code. Updates available at: http://www.courier-mta.org/?download.php **Debian:** **http://security.debian.org/pool/updates/main/c/courier** There is no exploit code required; however, a Proof of Concept exploit has been published.	SqWebMail HTML Email Arbitrary Code Execution CAN-2005-2724	Medium	Secunia Advisory: SA16600, August 29, 2005 **Debian Security Advisory, DSA 793-1, September 1, 2005**

Jonas Borgstrom Urban 1.5.3	Buffer overflow vulnerabilities have been reported in 'config/config.cc,' 'engine/game.cc,' 'highscor/highscor.cc,' and 'meny/meny.cc,' files when handling an overly long 'HOME' environment variable, which could let a malicious user execute arbitrary code with 'games' group privileges. Patches available at: http://www.freebsd.org/cgi/cvsweb.cgi/ports/games/urban A Proof of Concept exploit has been published.	Urban Multiple Buffer Overflows CAN-2005-2810	High	Security Tracker Alert ID: 1014848, September 3, 2005
KDE KDE 3.2.0 up to including 3.4.2	A vulnerability has been reported in 'kcheckpass.c' due to the insecure creation of the lock file, which could let a malicious user obtain superuser privileges. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/post-3.4.2-kdebase-kcheckpa ss.diff Mandriva: http://www.mandriva.com/security/advisories There is no exploit code required.	KDE kcheckpass Superuser Privilege Escalation CAN-2005-2494	High	KDE Security Advisory, September 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:160, September 6, 2005
KDE KDE 3.0 - 3.4.2	A vulnerability was reported in 'langen2kvtml' due to the insecure creation of temporary files, which could let malicious user obtain elevated privileges. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Mandriva: http://www.mandriva.com/security/advisories** There is no exploit code required.	KDE langen2kvtml Insecure Temporary File Creation CAN-2005-2101	Medium	KDE Security Advisory, August 15, 2005 Fedora Update Notification, FEDORA-2005-745, August 15, 2005 Fedora Update Notifications, FEDORA-2005-744 & 745, August 16, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:159, September 6, 2005**
man2web man2web 0.88, 0.87	A vulnerability has been reported in multiple scripts because a remote malicious user can submit arbitrary commands through HTTP GET requests, which could lead to the execution of arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however a, a Proof of Concept exploit script has been published.	Man2web Multiple Scripts Command Execution CAN-2005-2812	High	Security Focus, Bugtraq ID: 14747, September 6, 2005

MPlayer MPlayer 1.0 pre7, .0 pre6-r4, 1.0 pre6-3.3.5-20050130	A buffer overflow vulnerability has been reported due to insufficient validation of user-supplied strings, which could let a remote malicious user execute arbitrary code. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-01.xml** **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	MPlayer Audio Header Buffer Overflow CAN-2005-2718	High	Security Tracker Alert ID: 1014779, August 24, 2005 **Gentoo Linux Security Advisory, GLSA 200509-01, September 1, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:158, September 7, 2005**
Multiple Vendors Gentoo Linux 0.5, 0.7, 1.1 a, 1.2, 1.4, rc1-rc3; libdbi-perl libdbi-perl 1.21, 1.42	A vulnerability exists in libdbi-perl due to the insecure creation of temporary files, which could let a remote malicious user overwrite arbitrary files. Debian: http://security.debian.org/pool/updates/main/libd/libdbi-perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-069.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libd/libdbi-perl/ Mandrake: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:030 SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** There is no exploit code required.	Libdbi-perl Insecure Temporary File Creation CAN-2005-0077	Medium	Debian Security Advisory, DSA 658-1, January 25, 2005 Ubuntu Security Notice, USN-70-1, January 25, 2005 Gentoo Linux Security Advisory, GLSA 200501-38, January 26, 2005 RedHat Security Advisory, RHSA-2005:069-08, February 1, 2005 MandrakeSoft Security Advisory, MDKSA-2005:030, February 8, 2005 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005 **Fedora Update Notification, FEDORA-2005-841, September 6, 2005**

Multiple Vendors
Glyph and Cog Xpdf 3.0, pl2 & pl3; Ubuntu Linux 5.0 4 powerpc, i386, amd64;
RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0;
KDE 3.4.1, 3.4, 3.3.1, 3.3.2; GNOME GPdf 2.8.3, 2.1
	A remote Denial of Service vulnerability has been reported when verifying malformed 'loca' table in PDF files.
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-670.html
	http://rhn.redhat.com/errata/RHSA-2005-671.html
	http://rhn.redhat.com/errata/RHSA-2005-708.html
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/x/xpdf/
	KDE:
	http://www.kde.org/info/security/advisory-20050809-1.txt
	Mandriva:
	http://www.mandriva.com/security/advisories
	SGI:
	ftp://patches.sgi.com/support/free/security/advisories/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200508-08.xml
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Debian:
	http://security.debian.org/pool/updates/main/k/kdegraphics/
	Trustix:
	http://http.trustix.org/pub/trustix/updates/
	TurboLinux:
	ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/
	Currently we are not aware of any exploits for this vulnerability.
		XPDF Loca Table Verification Remote Denial of Service
		CAN-2005-2097
			Low	RedHat Security Advisories, RHSA-2005:670-05 & RHSA-2005:671-03, & RHSA-2005:708-05, August 9, 2005
				Ubuntu Security Notice, USN-163-1, August 09, 2005
				KDE Security Advisory, 20050809-1, August 9, 2005
				Mandriva Linux Security Update Advisories, MDKSA-2005:134, 135, 136 & 138, August 11, 2005
				SGI Security Advisory, 20050802-01-U, August 15, 2005
				Gentoo Linux Security Advisory GLSA, 200508-08, August 16, 2005
				Fedora Update Notifications, FEDORA-2005-729, 730, 732, & 733, August 15 & 17, 2005
				Debian Security Advisory, DSA 780-1, August 22, 2005
				Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005
				Turbolinux Security Advisory, TLSA-2005-88, September 5, 2005

Multiple Vendors SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12	A buffer overflow vulnerability has been reported in the XFRM network architecture code due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code. Patches available at: http://www.kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel XFRM Array Index Buffer Overflow CAN-2005-2456	High	Security Focus, 14477, August 5, 2005 Ubuntu Security Notice, USN-169-1, August 19, 2005 **SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005**

Multiple Vendors Trustix Secure Linux 3.0, 2.2, Secure Enterprise Linux 2.0, SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server for S/390 9.0, Linux Enterprise Server 9; 2.6-2.6.12 .4	A Denial of Service vulnerability has been reported due to a failure to handle malformed compressed files. Upgrades available at: http://www.kernel.org/ pub/linux/kernel/v2.6/ linux-2.6.12.5.tar.gz Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/ pub/SUSE Trustix: http://http.trustix.org/ pub/trustix/updates/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ZLib Null Pointer Dereference Denial of Service CAN-2005-2459	Low	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005

Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3 , 0.1-0.1.6 1, 0.0.1-0.0.6	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: ftp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml SUSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ Mandriva: http://www.mandriva.com/security/advisories OpenBSD: http://www.openbsd.org/errata.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ zsync: http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download Apple: http://docs.info.apple.com/article.html?artnum=302163 SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id = 35093&release_id=351848	Zlib Compression Library Buffer Overflow CAN-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005 Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 USCERT Vulnerability Note VU#680620, July 22, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Security Focus, Bugtraq ID: 14162, August 26, 2005

	Debian: **http://security.debian.org/pool/updates/main/z/zsync/** Currently we are not aware of any exploits for this vulnerability.		**Debian Security Advisor y, DSA 797-1, September 1, 2005**

Multiple Vendors zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input. Zlib: http://www.zlib.net/zlib-1.2.3.tar.gz Debian: http://security.debian.org/pool/updates/main/z/zlib/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ OpenBSD: http://www.openbsd.org/errata.html#libz2 Mandriva: http://www.mandriva.com/security/ advisories?name=MDKSA-2005:124 Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.323596 FreeBSD: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc SUSE: http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html Gentoo: http://security.gentoo.org/glsa/glsa-200507-28.xml http://security.gentoo.org/glsa/glsa-200508-01.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Apple: http://docs.info.apple.com/article.html?artnum=302163 TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 **Debian: http://security.debian.org/pool/updates/main/**	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CAN-2005-1849	Low	Security Focus, Bugtraq ID 14340, July 21, 2005 Debian Security Advisory DSA 763-1, July 21, 2005 Ubuntu Security Notice, USN-151-1, July 21, 2005 OpenBSD, Release Errata 3.7, July 21, 2005 Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005 Secunia, Advisory: SA16195, July 25, 2005 Slackware Security Advisory, SSA:2005-203-03, July 22, 2005 FreeBSD Security Advisory, SA-05:18, July 27, 2005 SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005 Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005 Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005 Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005 Turbolinux Security Advisory , TLSA-2005-83, August 18, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 **Debian Security Advisory, DSA 797-1, September 1, 2005**

	z/zsync/ Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Linux kernel 2.6.8 rc1-rc3, 2.6.8, 2.6.11 -rc2-rc4, 2.6.11	A Denial of Service vulnerability has been reported due to an error in the AIO (Asynchronous I/O) support in the "is_hugepage_only_range()" function. **SUSE:** **ftp://ftp.SUSE.com/ pub/SUSE** An exploit script has been published.	Linux Kernel Asynchronous Input/Output Local Denial of Service CAN-2005-0916	Low	Secunia Advisory, SA14718, April 4, 2005 **SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005**
Multiple Vendors Linux kernel 2.6-2.6.12 .1	A vulnerability has been reported due to insufficient authorization before accessing a privileged function, which could let a malicious user bypass IPSEC policies. Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/l/ This issue has been addressed in Linux kernel 2.6.13-rc7. **SUSE:** **ftp://ftp.SUSE.com/ pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPSec Policies Authorization Bypass CAN-2005-2555	Medium	Ubuntu Security Notice, USN-169-1, August 19, 2005 Security Focus, Bugtraq ID 14609, August 19, 2005 Security Focus, Bugtraq ID 14609, August 25, 2005 **SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005**
Multiple Vendors Linux kernel 2.6-2.6.12 .1	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to an error when handling key rings; and a Denial of Service vulnerability was reported in the 'KEYCTL_JOIN_SESSION_KEYRING' operation due to an error when attempting to join a key management session. Patches available at: http://kernel.org/pub/linux/ kernel/v2.6/snapshots/ patch-2.6.13-rc6-git 1.bz2 Ubuntu: : http://security.ubuntu.com/ ubuntu/pool/main/l/ **Trustix:** **http://http.trustix.org/ pub/trustix/updates/** There is no exploit code required.	Linux Kernel Management Denials of Service CAN-2005-2098 CAN-2005-2099	Low	Secunia Advisory: SA16355, August 9, 2005 Ubuntu Security Notice, USN-169-1, August 19, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005**
Multiple Vendors Nikto 1.35; N-Stealth Free Edition 5.8, Commercial Edition 5.8	A vulnerability has been reported in Stealth and Nikto, Web vulnerability scanners due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. N-Stalker has released updated versions; users should contact the vendor for information regarding obtaining updates.	Multiple Vendor Web Vulnerability Scanners HTML Injection CAN-2005-2860 CAN-2005-2861	Medium	Security Focus, Bugtraq ID: 14717, September 1, 2005

	Nikto has released an update advising users to be cautious when viewing HTML reports. There is no exploit code required.			
Multiple Vendors Novell Evolution 2.0.2-2.0.4; LibTIFF 3.6.1; sy Software Products CUPS 1.1.12-1.1.23, 1.1.10, 1.1.7, 1.1.6, 1.1.4 -5, 1.1.4-3, 1.1.4 -2, 1.1.4, 1.1.1, 1.0.4 -8, 1.0.4; Ubuntu 4.10, 5.04	A remote Denial of Service vulnerability has been reported due to insufficient validation of specific header values. Libtiff: http://freshmeat.net/redir/libtiff/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tiff/ Mandriva: http://www.mandriva.com/security/advisories **TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** A Proof of Concept exploit has been published.	LibTiff Tiff Image Header Remote Denial of Service CAN-2005-2452	Low	Security Focus Bugtraq ID 14417, July 29, 2005 Ubuntu Security Notice, USN-156-1, July 29, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:142, August 18, 2005 **Turbolinux Security Advisory , TLSA-2005-89, September 5, 2005**
Multiple Vendors RedHat Fedora Core3; **Ubuntu Linux 4.1 ppc, ia64, ia32;** **NTP NTPd 4.0-4.2 .0a**	A vulnerability has been reported in xntpd when started using the '-u' option and the group is specified by a string, which could let a malicious user obtain elevated privileges. Upgrade available at: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/i386 /ntp-4.2.0.a.20040617-5.FC3.i386.rpm **NTP: http://ntp.isc.org/Main/DownloadViaHTTP?file=ntp4/snapshots/ntp-dev/20 05/08/ntp-dev-4.2.0b-20050827.tar.gz** **Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/n/ntp/** **Debian: http://security.debian.org/pool/updates/main/n/ntp/** **Mandriva: http://www.mandriva.com/security/advisories** There is no exploit code required.	XNTPD Insecure Privileges CAN-2005-2496	Medium	Fedora Update Notification, FEDORA-2005-812, August 26, 2005 **Ubuntu Security Notice, USN-175-1, September 01, 2005** **Debian Security Advisory, DSA 801-1, September 5, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:156, September 6, 2005**
Multiple Vendors SILC Secure Internet Live Conferencing 1.0, 0.9.11-0.9.21; Gentoo Linux	A vulnerability has been reported due to the insecure creation of '/tmp' in 'silcd.c,' which could let a remote malicious user create/overwrite arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required.	SILC Server Insecure Temporary File Creation CAN-2005-2809	Medium	Security Focus, Bugtraq ID: 14716, September 1, 2005
Multiple Vendors Simpleproxy 3.0-3.2 , 2.2b;	A format string vulnerability has been reported when handling HTTP proxy replies, which could let a remote	Simpleproxy HTTP Proxy Reply Format	High	Debian Security Advisory, DSA 786-1, August 26, 2005

Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/simpleproxy/simpleproxy-3.4.tar.gz? download Debian: http://security.debian.org/pool/updates/main/s/simpleproxy/ Currently we are not aware of any exploits for this vulnerability.	String CAN-2005-1857		**US-CERT VU#139421**
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Rob Flynn Gaim 1.3.1, 1.3 .0, 1.2.1, 1.2 , 1.1.1 -1.1.4, 1.0-1.0.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Desktop 4.0, Advanced Workstation for the Itanium Processor 2.1, IA64	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported due to the way away messages are handled, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability has been reported due to an error when handling file transfers. Updates available at: http://gaim.sourceforge.net/downloads.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-589.html http://rhn.redhat.com/errata/RHSA-2005-627.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-06.xml SGI: ftp://patches.sgi.com/support/free/security/advisories/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.suse.com /pub/suse/ **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** A Proof of Concept exploit has been published for the buffer overflow vulnerability.	Gaim AIM/ICQ Protocols Buffer Overflow & Denial of Service CAN-2005-2102 CAN-2005-2103	High	RedHat Security Advisories, RHSA-2005:589-16 & RHSA-2005:627-11, August 9, 2005 Ubuntu Security Notice, USN-168-1, August 12, 2005 Gentoo Linux Security Advisory, GLSA 200508-06, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:139, August 16, 2005 Fedora Update Notifications, FEDORA-2005-750 & 751, August 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 **Slackware Security Advisory, SSA:2005-242-03, August 31, 2005**

Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6.10, rc2, 2.6.8, rc1	A remote Denial of Service vulnerability has been reported in the kernel driver for compressed ISO file systems when attempting to mount a malicious compressed ISO image. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ISO File System Remote Denial of Service CAN-2005-2457	Low	Ubuntu Security Notice, USN-169-1, August 19, 2005 **SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005**
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Trustix Secure Linux 3.0, 2.2, Trustix Secure Enterprise Linux 2.0; SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server 9; Linux kernel 2.6-2.6.12 .4	A Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions. Upgrades available at: http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.12.5.tar.gz Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ZLib Invalid Memory Access Denial of Service CAN-2005-2458	Low	SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005
Nokia Affix 3.0-3.2, 2.1-2.1.2, 2.0 -2.0.2	A vulnerability has been reported in the 'event_pin_code_request()' function due to an input validation error, which could let a remote malicious user inject arbitrary shell commands via a specially crafted Bluetooth device name. Patches available at: http://affix.sourceforge.net/patch_btsrv_affix_2_1_2 http://affix.sourceforge.net/patch_btsrv_affix_3_2_0 **Debian:** **http://security.debian.org/pool/updates/main/a/affix/** There is no exploit code required.	Nokia Affix BTSRV Device Name Remote Command Execution CAN-2005-2716	High	DMA 2005-0826a Advisory, August 26, 2005 **Debian Security Advisory, DSA 796-1, September 1, 2005**
OpenSSL Project OpenSSL 0.9.6, 0.9.6 a-0.9.6 m, 0.9.7c	A vulnerability exists due to the insecure creation of temporary files, which could possibly let a malicious user overwrite arbitrary files. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-15.xml Ubuntu: http://security.ubuntu.com/	OpenSSL Insecure Temporary File Creation CAN-2004-0975	Medium	Trustix Secure Linux Bugfix Advisory, TSL-2004-0050, September 30, 2004 Gentoo Linux Security Advisory, GLSA 200411-15, November 8, 2004 Ubuntu Security Notice, USN-24-1, November 11, 2004 Debian Security Advisory DSA-603-1, December 1,

	ubuntu/pool/main/o/openssl/ Debian: http://www.debian.org/security/2004/dsa-603 Mandrakesoft: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:147 TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ FedoraLegacy: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-476.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-170.pdf** There is no exploit code required.			2004 Mandrakesoft Security Advisory, MDKSA-2004:147, December 6, 2004 Turbolinux Security Announce-ment, 20050131, January 31, 2005 SGI Security Advisory, 20050602-01-U, June 23, 2005 **Avaya Security Advisory, ASA-2005-170, August 29, 2005**
Padl Software pam_ldap Build 179, Build 169	A vulnerability has been reported when handling a new password policy control, which could let a remote malicious user bypass authentication policies. Upgrades available at: ftp://ftp.padl.com/pub/pam_ldap.tgz **Gentoo: http://security.gentoo.org/glsa/glsa-200508-22.xml** There is no exploit code required.	PADL Software PAM_LDAP Authentication Bypass CAN-2005-2641	Medium	Bugtraq ID: 14649, August 24, 2005 US-CERT VU#778916 **Gentoo Linux Security Advisory, GLSA 200508-22, August 31, 2005**

PCRE PCRE 6.1, 6.0, 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available at: http://www.pcre.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/pcre3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-17.xml Mandriva: http://www.mandriva.com/security/advisories **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/** **Debian:** **http://security.debian.org/pool/updates/main/p/pcre3/** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	PCRE Regular Expression Heap Overflow CAN-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 Ubuntu Security Notices, USN-173-1 & 173-2, August 24, 2005 Fedora Update Notifications, FEDORA-2005-802 & 803, August 24, 2005 Gentoo Linux Security Advisory, GLSA 200508-17, August 25, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:151-155, August 25, 26, & 29, 2005 **SUSE Security Announcements, SUSE-SA:2005:048 & 049, August 30, 2005** **Slackware Security Advisories, SSA:2005-242-01 & 242-02 , August 31, 2005** **Ubuntu Security Notices, USN-173-3, 173-4 August 30 & 31, 2005** **Debian Security Advisory, DSA 800-1, September 2, 2005** **SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005**
PolyGen PolyGen 1.0.6	A Denial of Service vulnerability has been reported due to resource exhaustion. Debian: http://security.debian.org/pool/updates/main/p/polygen/ Currently we are not aware of any exploits for this vulnerability.	PolyGen Denial of Service CAN-2005-2656	Low	Debian Security Advisory, DSA 794-1, September 1, 2005
ProFTPd	Multiple format string vulnerabilities have been reported in ProFTPd that could let remote malicious users cause a Denial of Service or disclose information. Upgrade to version 1.3.0rc2: http://www.proftpd.org/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200508-02.xml Trustix:	ProFTPD Denial of Service or Information Disclosure CAN-2005-2390	Medium	Secunia, Advisory: SA16181, July 26, 2005 Gentoo Linux Security Advisory, GLSA 200508-02, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Turbolinux Security Advisory, TLSA-2005-82, August 9, 2005

	ftp://ftp.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/p/proftpd/** **OpenPKG:** **ftp://ftp.openpkg.org/release/** Currently we are not aware of any exploits for these vulnerabilities.			Mandriva Linux Security Update Advisory, MDKSA-2005:140, August 16, 2005 **Debian Security Advisories, DSA 795-1 & 795-2, September 1, 2005** **OpenPKG Security Advisory, OpenPKG-SA-2005.020, September 6, 2005**
pstotext V1.9	A vulnerability has been reported in pstotext ('-dSAFER') that could let malicious users execute arbitrary postscript code. **Debian:** **http://security.debian.org/pool/updates/main/p/pstotext/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200507-29.xml** There is no exploit code required.	pstotext Arbitrary Code Execution **CAN-2005-2536**	High	Secunia, Advisory: SA16183, July 25, 2005 **Debian Security Advisory, DSA 792-1, August 31, 2005** **Gentoo Linux Security Advisory, GLSA 200507-29, August 31, 2005**
Smb4k Smb4k 0.4-0.6	A vulnerability has been reported due to the insecure creation of temporary files, which could let a malicious user obtain sensitive information. Patches available at: http://download.berlios.de/smb4k/001_security_fix_smb4k_0.4.1a.diff.gz Upgrades available at: http://download.berlios.de/smb4k/smb4k-0.6.3.tar.gz Mandriva: http://www.mandriva.com/security/advisories There is no exploit code required.	Smb4k Insecure Temporary File Creation CAN-2005-2851	Medium	Security Focus, Bugtraq ID: 14756, September 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:157, September 6, 2005
Squid Web Proxy Squid Web Proxy Cache 2.5 .STABLE1-STABLE 10, 2.4 .STABLE6 & 7, STABLE 2, 2.4, 2.3 STABLE 4&5, 2.1 Patch 2, 2.0 Patch 2	A remote Denial of Service vulnerability has been reported in '/squid/src/ssl.c' when a malicious user triggers a segmentation fault in the 'sslConnectTimeout()' function. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE10-sslConnectTimeout.patch There is no exploit code required.	Squid 'sslConnect Timeout()' Remote Denial of Service CAN-2005-2796	Low	Security Tracker Alert ID: 1014846, September 2, 2005
University of Minnesota gopherd 3.0.9	A buffer overflow vulnerability has been reported in the 'VlfromLine()' function when copying an input line, which	UMN Gopher Client Remote Buffer Overflow	Medium	Secunia Advisory: SA16614, August 30, 2005

	could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. An exploit script has been published.	CAN-2005-2772		**US-CERT VU#619812**
Vim V6.3.082	A vulnerability has been reported in Vim that could let remote malicious users execute arbitrary code. Vendor patch available: ftp://ftp.vim.org/pub/vim/patches/6.3/6.3.082 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/v/vim/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-745.html **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-189.pdf** There is no exploit code required; however, Proof of Concept exploits have been published.	Vim Arbitrary Code Execution CAN-2005-2368	High	Security Focus, 14374, July 25, 2005 Ubuntu Security Notice, USN-154-1, July 26, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0038, July 29, 2005 Fedora Update Notifications, FEDORA-2005-737, 738, & 741, August 10 & 15, 2005 Conectiva Security Advisory, CLSA-2005:995, Mandriva Linux Security Update Advisory, MDKSA-2005:148, August 22, 2005 RedHat Security, Advisory, RHSA-2005:745-10, August 22, 2005 **Avaya Security Advisory, ASA-2005-189-, August 31, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source

Barracuda Networks Barracuda Spam Firewall 3.1.17 firmware	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in 'IMG.PL' which could let a remote malicious user obtain sensitive information; and a vulnerability was reported when user-supplied commands are submitted to the web interface, which could let a remote malicious user execute arbitrary commands. The vendor has released firmware version 3.1.18 to address this and other issues. Please contact the vendor to obtain the upgrade. There is no exploit code required; however, Proofs of Concept exploits have been published.	Barracuda Spam Firewall Remote Directory Traversal & Remote Command Execution CAN-2005-2847 CAN-2005-2848 CAN-2005-2849	High	Security Focus, Bugtraq ID: 14710 & 14712, September 1, 2005
Cisco Systems Cisco IOS 12.2ZH & 12.2ZL based trains, 12.3 based trains, 12.3T based trains, 12.4 based trains, 12.4T based trains	A buffer overflow vulnerability has been reported in the authentication proxy, which could let a remote malicious user cause a Denial of Service or potentially execute arbitrary code. Patch information available at: http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco IOS Firewall Authentication Proxy Buffer Overflow CAN-2005-2841	High	Cisco Security Advisory, Document ID: 66269, September 7, 2005 US-CERT VU#236045
CMS Made Simple CMS Made Simple 0.10	Several vulnerabilities have been reported: a vulnerability was reported in the 'admin/lang.php' script due to insufficient authentication, which could let a remote malicious user bypass authentication procedures; and a vulnerability was reported in 'admin/lang.php' due to insufficient verification of the 'nls[file][vx][vxsfx]' parameter, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	CMS Made Simple Authentication Bypass & File Include CAN-2005-2846	High	Secunia Advisory: SA16654, September 1, 2005
EMC Software NetWorker 6.x, 7.1.3, 7.2; Sun StorEdge Enterprise Backup Software 7.0-7.2, Solstice Backup Software 6.0, 6.1	Several vulnerabilities have been reported: a vulnerability was reported in 'AUTH_UNIX' due to weak authentication, which could let a remote malicious user execute arbitrary commands, view/modify configuration, cause a Denial of Service, or obtain sensitive information; a vulnerability was reported due to insufficient authentication of tokens, which could let a remote malicious user execute arbitrary commands as ROOT; and a vulnerability was reported in the Legato PortMapper because any host can call 'pmap_set' and 'pmap_unset,' which could let a remote malicious user cause a Denial of Service or eavesdrop on NetWorker process communications. Patch information available at: http://www.legato.com/support/websupport/product_alerts/081605_NW_authentication.htm http://www.legato.com/support/websupport/product_alerts/081605_NW_token_authentication.htm http://www.legato.com/support/websupport/product_alerts/081605_NW_port_mapper.htm **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-101886-1** There is no exploit code required.	EMC Legato NetWorker Multiple Vulnerabilities CAN-2005-0357 CAN-2005-0358 CAN-2005-0359	High	US-CERT VU#606857 US-CERT VU#407641 US-CERT VU#801089 Sun(sm) Alert Notification Sun Alert ID: 101886, August 17, 2005 **Sun(sm) Alert Notification** **Sun Alert ID: 101886, Updated, September 1, 2005**
Eric Fichot DownFile 1.3	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'email.php,' 'index.php,'and 'del.php' due to insufficient sanitization of the 'id' parameter and in 'add_form.php' due to insufficient sanitization	DownFile Cross-Site Scripting &	High	Secunia Advisory: SA16630, September 1, 2005

	of the 'mode' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because it is possible to access the administration section without authentication. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Authentication Bypass CAN-2005-2818 CAN-2005-2819		
Ethereal Ethereal V0.10.11	Multiple dissector and zlib vulnerabilities have been reported in Ethereal that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version 0.10.12: http://www.ethereal.com/download.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-687.html SUSE: ftp://ftp.suse.com/pub/suse/ **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-185.pdf** Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Denial of Service or Arbitrary Code Execution CAN-2005-2361 CAN-2005-2362 CAN-2005-2363 CAN-2005-2364 CAN-2005-2365 CAN-2005-2366 CAN-2005-2367	High	Secunia, Advisory: SA16225, July 27, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:131, August 4, 2005 RedHat Security Advisory, RHSA-2005:687-03, August 10, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 **Avaya Security Advisory, ASA-2005-185, August 30, 2005**
FlatNuke FlatNuke 2.5.6	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported in 'index.php' due to insufficient verification of the 'ID' parameter, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the 'USR' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	FlatNuke Directory Traversal & Cross-Site Scripting CAN-2005-2813 CAN-2005-2814 CAN-2005-2815	Medium	Security Focus Bugtraq ID: 14702 & 14704 August 31, 2005
gBook gBook 1.0.1, 1.0	Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of unspecified input before returned to user, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/gbook/gbook-1.0.2.tar.gz?download There is no exploit code required.	GBook Multiple Cross-Site Scripting	Medium	Secunia Advisory: SA16668, September 2, 2005
GuppY GuppY 4.5.3 a, 4.5.3, 4.5	Several vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'printfaq.php' due to insufficient sanitization of the 'pg' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the 'Referer' and 'User-Agent' HTTP headers, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.freeguppy.org/file/gy_upg_454.zip There is no exploit code required.	GuppY Cross-Site Scripting CAN-2005-2853	Medium	Secunia Advisory: SA16707, September 6, 2005

Hewlett Packard Company Proliant DL585 Server, Integrated Lights Out 1.80	A vulnerability has been reported because when the server is powered down a remote malicious user can obtain unauthorized access. **Rev 1: Updated Summary, Resolution, and updated next release from V1.81 to V1.82** Updates available at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBMA01220 Currently we are not aware of any exploits for this vulnerability.	HP Proliant DL585 Server Unauthorized Remote Access CAN-2005-2552	Medium	HP Security Bulletin, HPSBMA01220, August 11, 2005 **HP Security Bulletin, HPSBMA01220, Rev. 1, September 1, 2005**
Hewlett Packard Company OpenView Event Correlation Services 3.31-3.33 Windows, 3.31-3.33 Solaris, 3.31-3.33 Linux, 3.31-3.33 HP-UX	A vulnerability has been reported in the 'cgi-bin/ecscmg.ovpl' script due to insufficient validation of user-supplied input before using as part of a system command, which could let a remote malicious user obtain elevated privileges. As a workaround, the vendor indicates that you can move the 'ecscmg.ovpl' file from the cgi-bin directory into another directory. The directory should not have write permissions for ordinary users. Currently we are not aware of any exploits for this vulnerability.	HP OpenView Event Correlation Services Remote Elevated Privileges	Medium	HP Security Bulletin, HPSBMA01225, September 4, 2005
Ilia Alshanetsky FUDForum 2.6.15	A vulnerability has been reported in the 'mid' parameter due to insufficient validation before retrieving a forum post, which could let a remote malicious user bypass certain security restrictions and obtain sensitive information. PHPGroupWare: http://prdownloads.sourceforge.net/phpgroupware/phpgroupware-0.9.16.00 7.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200508-20.xml **Debian:** **http://security.debian.org/pool/updates/main/p/phpgroupware/** There is no exploit code required.	FUDForum Security Restriction Bypass CAN-2005-2600	Medium	Secunia Advisory: SA16414, August 12, 2005 Security Focus, Bugtraq ID: 14556, August 25, 2005 Gentoo Linux Security Advisory, GLSA 200508-20, August 30, 2005 **Debian Security Advisory , DSA 798-1, September 2, 2005**
MAXdev MD-Pro 1.0.72	Cross-Site Scripting vulnerabilities have been reported in the 'dl-search.php' and 'wl-search.php' scripts due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in the 'Downloads' section because it is possible to upload files that contain arbitrary file extensions. Upgrade available at: http://www.maxdev.com/Downloads-index-req-viewdownload-cid-3.phtml There is no exploit code required; however, detailed exploitation has been published.	MAXdev MD-Pro Cross-Site Scripting & File Upload CAN-2005-2839	Medium	Secunia Advisory: SA16731, September 7, 2005
Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'InstallTrigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error	Firefox Multiple Vulnerabilities CAN-2005-2260 CAN-2005-2261 CAN-2005-2262 CAN-2005-2263 CAN-2005-2264 CAN-2005-2265 CAN-2005-2267 CAN-2005-2269 CAN-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications,

	when handling DOM node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/ Gentoo: ftp://security.gentoo.org/glsa/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-586.html Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/epiphany-browser/ http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ http://security.debian.org/pool/updates/main/m/mozilla/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-24.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla-firefox/** Exploits have been published.		FEDORA-2005-603 & 605, July 20, 2005 RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July 22, 2005 US-CERT VU#652366 US-CERT VU#996798 Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 SUSE Security Announcement, SUSE-SA:2005:045, August 11, 2005 Debian Security Advisory, DSA 775-1, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Debian Security Advisory, DSA 777-1, August 17, 2005 Debian Security Advisory, DSA 779-1, August 20, 2005 Debian Security Advisory, DSA 781-1, August 23, 2005 Gentoo Linux Security Advisory, GLSA 200507-24, August 26, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:127-1, August 26, 2005 Slackware Security Advisory, SSA:2005-085-01, August 28, 2005 **Debian Security Advisory, DSA 779-2, September 1, 2005**

Multiple Vendors PHPGroupWare 0.9.16.000; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	A vulnerability has been reported because an authenticated administrator can edit the main screen messages to include arbitrary HTML, which could let a remote malicious user with administrative privileges inject arbitrary HTML. Upgrades available at: http://prdownloads.sourceforge.net/phpgroupware/phpgroupware-0.9.16.00 7.tar.gz Debian: http://security.debian.org/pool/updates/main/p/phpgroupware/ There is no exploit code required.	PHPGroupWare Main Screen Message Script Injection CAN-2005-2761	Medium	Security Tracker Alert ID: 1014832, September 1, 2005 Debian Security Advisory, DSA 798-1, September 2, 2005
Multiple Vendors Squid Web Proxy Cache2.5. STABLE9 & prior	A vulnerability has been reported in the DNS client when handling DNS responses, which could let a remote malicious user spoof DNS lookups. Patch available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE9-dns_query-4.patch Trustix: http://www.trustix.org/errata/2005/0022/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-415.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI: http://www.sgi.com/support/security/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.	Squid Proxy DNS Spoofing CAN-2005-1519	Medium	Security Focus, 13592, May 11, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005 Fedora Update Notification, FEDORA-2005-373, May 17, 2005 Ubuntu Security Notice, USN-129-1 May 18, 2005 RedHat Security Advisory, RHSA-2005:415-16, June 14, 2005 Turbolinux Security Advisory, TLSA-2005-71, June 28, 2005 SGI Security Advisory, 20050605-01-U, July 12, 2005 **Conectiva Linux Announcement, CLSA-2005:1000, August 31, 2005**
Multiple Vendors Windows XP, Server 2003 Windows Services for UNIX 2.2, 3.0, 3.5 when running on Windows 2000 Berbers V5 Release 1.3.6 AAA Intuit LX, Converged Communications Server (CCS) 2.x, MN100, Modular Messaging 2.x, S8XXX Media Servers	An information disclosure vulnerability has been reported that could let a remote malicious user read the session variables for users who have open connections to a malicious telnet server. Updates available: http://www.microsoft.com/tech net/security/Bulletin/MS05-033.mspx RedHat: ftp://updates.redhat.com/enterprise Microsoft: http://www.microsoft.com/tech net/security/Bulletin/MS05-033.mspx SUSE: ftp://ftp.SUSE.com/pub/SUSE AAA: http://support.avaya.com/elmodocs2/security/	Multiple Vendor Telnet Client Information Disclosure CAN-2005-1205 CAN-2005-0488	Medium	Microsoft, MS05-033, June 14, 2004 US-CERT VU#800829 iD EFENSE Security Advisory, June 14, 2005 Red Hat Security Advisory, RHSA-2005:504-00, June 14, 2005 Microsoft Security Bulletin, MS05-033 & V1.1, June 14 & 15, 2005 SUSE Security Summary Report, SUSE-SR:2005:016,

	ASA-2005-145 RHSA-2005-504.pdf Trustix: ftp://ftp.turbolinux.co.jp/ pub/TurboLinux/ TurboLinux/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-567.html SGI: ftp://oss.sgi.com/projects/ sgi_propack/download/3/ updates/ Mandriva: http://www.mandriva.com/ security/advisories Microsoft: Bulletin revised to communicate the availability of security updates for Services for UNIX 2.0 and Services for UNIX 2.1. The “Security Update Information” section has also be revised with updated information related to the additional security updates. F5: http://tech.f5.com/home/ bigip/solutions/ advisories/ sol4616.html **SCO:** **ftp://ftp.sco.com/pub/ updates/UnixWare/ SCOSA-2005.35** Currently we are not aware of any exploits for this vulnerability.			June 17, 2005 AAA Security Advisory, ASA-2005-145, June 17, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 RedHat Security Advisory, RHSA-2005:567-08, July 12, 2005 SGI Security Advisories, 20050605-01-U, 20050702-01-U, & 20050703-01-U, July 12 & 15, 2005 Microsoft Security Bulletin, MS05-033 V2.0 July 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:119, July 14, 2005 **SCO Security Advisory, SCOSA-2005.35, September 1, 2005**
Multiple Vendors Gentoo Linux; Apache Software Foundation Apache 2.1-2.1.5, 2.0.35-2.0.54, 2.0.32, 2.0.28, Beta, 2.0 a9, 2.0	A remote Denial of Service vulnerability has been reported in the HTTP 'Range' header due to an error in the byte-range filter. Patches available at: http://issues.apache.org/ bugzilla/attachment.cgi ?id=16102 Gentoo: http://security.gentoo.org/ glsa/glsa-200508-15.xml **RedHat:** **http://rhn.redhat.com/ errata/RHSA-2005-608.html** There is no exploit code required.	Apache Remote Denial of Service CAN-2005-2728	Low	Secunia Advisory: SA16559, August 25, 2005 Security Advisory, GLSA 200508-15, August 25, 2005 **RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005**
Multiple Vendors OpenTTD 0.4.0.1; Gentoo Linux	Multiple format string vulnerabilities have been reported in 'network_server.c,' 'network.c,' 'console_cmds.c,' and 'network_client.c' due to the way text messages are handled, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code; and a vulnerability was reported in 'vsprint()' due to boundary errors, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. Gentoo: http://security.gentoo.org/ glsa/glsa-200509-03.xml Currently we are not aware of any exploits for this vulnerability.	OpenTTD Multiple Format Strings CAN-2005-2763	High	Gentoo Linux Security Advisory,GLSA 200509-03, September 5, 2005

Multiple Vendors PHPXMLRPC 1.1.1; PEAR XML_RPC 1.3.3; Drupal 4.6-4.6.2, 4.5- 4.5.4; Nucleus CMS Nucleus CMS 3.21, 3.2, 3.1, 3.0, RC, 3.0.; MailWatch for MailScanner 1.0.1; eGroupWare 1.0.6, 1.0.3, 1.0.1, 1.0.0.007, 1.0	A vulnerability has been reported in XML-RPC due to insufficient sanitization of certain XML tags that are nested in parsed documents being used in an 'eval()' call, which could let a remote malicious user execute arbitrary PHP code. PHPXMLRPC : http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc.1.2.tgz?download Pear: http://pear.php.net/get/XML_RPC-1.4.0.tgz Drupal: http://drupal.org/files/projects/drupal-4.5.5.tar.gz eGroupWare: http://prdownloads.sourceforge.net/egroupware/eGroupWare-1.0.0.009.tar .gz?download MailWatch: http://prdownloads.sourceforge.net/mailwatch/mailwatch-1.0.2.tar.gz Nucleus: http://prdownloads.sourceforge.net/nucleuscms/nucleus-xmlrpc-patch.zip ?download RedHat: http://rhn.redhat.com/errata/RHSA-2005-748.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200508-13.xml http://security.gentoo.org/glsa/glsa-200508-14.xml http://security.gentoo.org/glsa/glsa-200508-18.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/p/php4/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200508-20.xml** **http://security.gentoo.org/glsa/glsa-200508-21.xml** **Slackware:** **ftp://ftp.slackware.com/**	PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution CAN-2005-2498	High	Security Focus, Bugtraq ID 14560, August 15, 2995 Security Focus, Bugtraq ID 14560, August 18, 2995 RedHat Security Advisory, RHSA-2005:748-05, August 19, 2005 Ubuntu Security Notice, USN-171-1, August 20, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:146, August 22, 2005 Gentoo Linux Security Advisory, GLSA 200508-13 & 14, & 200508-18, August 24 & 26, 2005 Fedora Update Notifications, FEDORA-2005-809 & 810, August 25, 2005 Debian Security Advisory, DSA 789-1, August 29, 2005 SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005 **Gentoo Linux Security Advisory, GLSA GLSA 200508-20& 200508-21, August 30 & 31, 2005** **Slackware Security Advisory, SSA:2005-242-02, August 31, 2005** **Debian Security Advisory, DSA 798-1, September 2, 2005** **SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005**

	pub/slackware/ **Debian:** **http://security.debian.org/pool/updates/main/p/phpgroupware/** There is no exploit code required.			
MyBB Group MyBulletinBoard RC1-RC4, PR2	A Cross-Site Scripting vulnerability has been reported in 'Forumdisplay.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	MyBulletinBoard Cross-Site Scripting	Medium	Security Focus Bugtraq ID: 14754, September 6, 2005
myWebland myBloggie 2.1.1-2.1.3	An SQL injection vulnerability has been reported in 'login.php' due to insufficient sanitization of the 'username' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Patches available at: http://mywebland.com/downloads/login.php There is no exploit code required.	MyBloggie SQL Injection CAN-2005-2838	Medium	Secunia Advisory: SA16699, September 5, 2005
Noah Grey GreyMatter 1.3.1	A Cross-Site Scripting vulnerability has been reported in 'Gm.CGI' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Greymatter Cross-Site Scripting CAN-2005-2816	Medium	Security Focus, Bugtraq ID: 14703, August 31, 2005
Novell Netware 6.5 SP2&3, 6.0, SP1-SP3, 5.1, SP4&5	A remote Denial of Service vulnerability has been reported in 'CIFS.NLM' when handling password lengths. Patches available at: http://support.novell.com/servlet/filedownload/sec/pub/cifspt9.exe W32.Randex.CCC exploits this vulnerability.	Novell Netware CIFS.NLM Denial of Service CAN-2005-2852	Low	Novell Technical Information Documents, TID2971821, 1822, 1832, August 30, 2005
Novell NetMail 3.52-3.52 B, 3.10, a-h, 3.1 f, 3.1, 3.0.3, a&b, 3.0.1	A buffer overflow vulnerability has been reported in the IMAP command continuation function due to insufficient boundary checks, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://support.novell.com/servlet/filedownload/sec/pub/ Currently we are not aware of any exploits for this vulnerability.	Novell NetMail Remote IMAP Buffer Overflow CAN-2005-1758	High	Security Focus, Bugtraq ID: 14718, September 1, 2005
OpenSSH OpenSSH 4.1, 4.0, p1	Several vulnerabilities have been reported: a vulnerability was reported due to an error when handling dynamic port forwarding when no listen address is specified, which could let a remote malicious user cause "GatewayPorts" to be incorrectly activated; and a vulnerability was reported due to an error when handling GSSAPI credential delegation, which could let a remote malicious user be delegated with GSSAPI credentials. Upgrades available at: ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-4.2.tar.gz Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ There is no exploit code required.	OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials CAN-2005-2797 CAN-2005-2798	Medium	Secunia Advisory: SA16686, September 2, 2005 Fedora Update Notification, FEDORA-2005-858, September 7, 2005
PBLang PBLang 4.66, 4.65, 4.63, 4.56 (4.5 RC 2), 4.6, 4.0	Several vulnerabilities have been reported: a vulnerability was reported because restricted forums can be accessed without proper permissions, a vulnerability was reported in 'register.php' and 'ucp.php' due to unspecified errors, which could let a remote malicious user obtain administrative privileges; and a vulnerability was reported because authenticated remote malicious users can delete private messages. Upgrades available at:	PBLang Multiple Vulnerabilities	High	Security Focus, Bugtraq ID: 14728, September 2, 2005

	http://prdownloads.sourceforge.net/pblang/PBL466z.zip?download There is no exploit code required.			
Phorum Phorum 5.0.10-5.0.17 a	A Cross-Site Scripting vulnerability has been reported in 'register.php' due to insufficient sanitization of the 'username' field, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://phorum.org/ There is no exploit code required.	Phorum Cross-Site Scripting CAN-2005-2836	Medium	Secunia Advisory: SA16667, September 2, 2005
Plain Black Software WebGUI 6.7.0-6.7.2, 6.6.x, 6.5.x, 6.4.x, 6.3.x, 6.2-6.2.9 , 5.2.4, 5.2.3	Several vulnerabilities have been reported in 'Help.pm,' 'International.pm,' and 'WebGUI.pm' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary Perl code. Upgrades available at: http://prdownloads.sourceforge.net/pbwebgui/webgui-6.7.3-gamma.tar.gz? download There is no exploit code required.	Plain Black Software WebGUI Remote Perl Command Execution CAN-2005-2837	High	Security Focus Bugtraq ID: 14732, September 2, 2005
Simple Machines SMF 1.0.5	A vulnerability has been reported because external files can be used as avatars, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	SMF Avatar Image Implementation Information Disclosure CAN-2005-2817	Medium	Security Tracker Alert ID: 1014828, August 31, 2005
Sun Micro-systems, Inc. Java Web Start 1.x, Sun Java JDK 1.5.x, 1.4.x, Sun Java JRE 1.4.x, 1.5.x	Several vulnerabilities have been reported: a vulnerability was reported due to an unspecified error which could let malicious untrusted applications execute arbitrary code; and a vulnerability was reported due to an unspecified error which could let a malicious untrusted applets execute arbitrary code. Upgrades available at: http://java.sun.com/j2se/1.5.0/index.jsp http://java.sun.com/j2se/1.4.2/download.html Slackware: ftp://ftp.slackware.com/pub/slackware/slackware-current/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **HP:** **http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBUX01214** Currently we are not aware of any exploits for these vulnerabilities.	Java Web Start / Sun JRE Sandbox Security Bypass CAN-2005-1973 CAN-2005-1974	High	Sun(sm) Alert Notification, 101748 & 101749, June 13, 2005 Slackware Security Advisory, SSA:2005-170-01, June 20, 2005 SUSE Security Announce-ment, SUSE-SA:2005:032, June 22, 2005 **HP Security Bulletin, HPSBUX01214, August 29, 2005**
Sun Microsystems, Inc. Sun Java JRE 1.3.x, 1.4.x, Sun Java SDK 1.3.x, 1.4.x; Conectiva Linux 10.0; Gentoo Linux; HP HP-UX B.11.23, B.11.22, B.11.11, B.11.00, HP Java SDK/RTE for HP-UX PA-RISC 1.3, HP Java SDK/RTE for HP-UX PA-RISC	A vulnerability exists due to a design error because untrusted applets for some private and restricted classes used internally can create and transfer objects, which could let a remote malicious user turn off the Java security manager and disable the sandbox restrictions for untrusted applets. Updates available at: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57591-1 Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Gentoo: http://security.gentoo.org/	Sun Java Plug-in Sandbox Security Bypass CAN-2004-1029	Medium	Sun(sm) Alert Notification, 57591, November 22, 2004 US-CERT Vulnerability Note, VU#760344, November 23, 2004 Conectiva Linux Security Announcement, CLA-2004:900, November 26, 2004 Gentoo Linux Security Advisory, GLSA

1.4; Symantec Gateway Security 5400 Series v2.0.1, v2.0, Enterprise Firewall v8.0	glsa/glsa-200411-38.xml HP: http://www.hp.com/go/java Symantec: http://securityresponse.symantec.com/avcenter/security/Content/2005.01.04.html SuSE: ftp://ftp.suse.com/pub/suse/ **HP:** **http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBUX01214** Currently we are not aware of any exploits for this vulnerability.			200411-38, November 29, 2004 HP Security Bulletin, HPSBUX01100, December 1, 2004 Sun(sm) Alert Notification, 57591, January 6, 2005 (Updated) Symantec Security Response, SYM05-001, January 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:002, January 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 **HP Security Bulletin, HPSBUX01214, August 29, 2005**
thesitewizard.com chfeedback.pl Feedback Form Perl Script 2.0.1	A vulnerability has been reported because the application can be used as a mail relay, which could let a remote malicious user inject arbitrary SMTP headers. Users are advised to contact the vendor for an update. There is no exploit code required.	Feedback Form Perl Script CHFeedBack.PL Mail Relay CAN-2005-2854	Medium	Security Focus, Bugtraq ID: 14749, September 6, 2005
Unclassified NewsBoard Unclassified NewsBoard 1.5.3	A vulnerability has been reported in the Description field due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Unclassified NewsBoard Description Field HTML Injection CAN-2005-2855	Medium	Security Focus, Bugtraq ID: 14748, September 6, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Mobile users clueless on data:** According to a survey conducted by mobile software company, SurfKitchen, not one mobile phone user could correctly identify the data package on their phone. The survey found that perceived high prices, poor usability and unreliability of service were the main reasons for customers shunning data services. Source: http://www.vnunet.com/vnunet/news/2141987/mobile-users-clueless.
- **F-Secure: Commwarrior claims first big victim:** According to an F-Secure security expert, a mobile phone virus, Commwarrior.B is the first mobile virus that has infected an organization. "It's a particularly nasty version of Commwarrior, as it just doesn't give up." Source: http://news.com.com/F-Secure+Commwarrior+claims+first+big+victim/2100-7349_3-845021.html?part=rss&tag=5845021&subj=news .
- **Vendors Claim Mobile Viruses Worsening:** Both F-Secure and Trend Micro, mobile anti-virus product vendors, claim that attacks on mobile devices are becoming more serious. Virus that have been reported attack Symbian-based devices. During July, three new viruses and five new variants of existing viruses appeared. Source: http://www.securitypipeline.com/news/170102188.

Wireless Vulnerabilities

- Nokia Affix BTSRV Device Name Remote Command Execution: An input validation vulnerability has been reported which could let a remote malicious user inject arbitrary shell commands. Updated information regarding Debian patch.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse	Script name	Workaround or Patch	Script Description

Chronological Order)		Available	
September 7, 2005	dl-cups.c	Yes	Denial of Service exploit for the CUPs 1.x vulnerability.
September 7, 2005	draft-gont-tcpm-icmp-attacks-04.txt	N/A	A document that discusses the use of the Internet Control Message Protocol (ICMP) to perform a variety of attacks against the Transmission Control Protocol (TCP) and other similar protocols.
September 7, 2005	freeSMTP.pl.txt	No	Proof of Concept exploit for the Free SMTP Server As Open Relay vulnerability.
September 7, 2005	MAXdevMD-Pro1.0.73.txt	Yes	Detailed exploitation for the MAXdev MD-Pro Cross-Site Scripting & File Upload vulnerabilities.
September 7, 2005	ms05-018.c	Yes	Exploit for the Microsoft Windows Kernel CSRSS Local Privilege Escalation vulnerability.
September 7, 2005	MSRC-6005bgs-EN.txt keybd.c	No	Proof of Concept exploits for the Microsoft Windows Keyboard Event Privilege Escalation vulnerability.
September 7, 2005	phpcal.txt	No	Exploit details for the phpCommunityCalendar Multiple vulnerabilities.
September 7, 2005	realchat_PoC.tgz	No	Proof of Concept exploit for Realchat user impersonation vulnerability.
September 7, 2005	stealth_1.34.tar.gz	N/A	Stealth (SSH-based Trust Enhancement Acquired through a Locally Trusted Host) is a file integrity scanner.
September 7, 2005	urbanGame.txt	Yes	Proof of Concept exploit for the Urban Multiple Buffer Overflows vulnerability.
September 6, 2005	dl-mancgi.c	No	Proof of Concept exploit for the Man2web Multiple Scripts Command Execution vulnerability.
September 2, 2005	FileZilla_pass.c	No	Proof of Concept exploit for the FileZilla FTP Client Hard-Coded Cipher Key vulnerability.
September 1, 2005	cpanel-9x_RCE.c	No	Exploit for cPanel Remote Command Execution vulnerability.
September 1, 2005	SlimFTPd-RemoteDoS.c	No	Exploit for the WhitSoft Development SlimFTPd Remote Denial of Service vulnerability.
August 31, 2005	0508-exploits.tgz	N/A	New Packet Storm exploits for August, 2005.
August 31, 2005	AD20050830.txt	No	Exploit for the BNBT EasyTracker Remote Denial Of Service vulnerability.
August 31, 2005	dameware.c	Yes	Script that exploits the DameWare Arbitrary Code Execution vulnerability.
August 31, 2005	flat256.html flatnuke256.txt	No	Detailed exploitation for the FlatNuke Directory Traversal & Cross-Site Scripting vulnerabilities.
August 31, 2005	fud.html	No	Remote code execution exploit for FUD Forum Upload Arbitrary Script vulnerability.
August 31, 2005	HP_OV_NNM_RCE.c	Yes	Script that exploits the HP OpenView Network Node Manager Remote Arbitrary Code Execution vulnerability.
August 31, 2005	lduSQL.txt	No	Exploitation details for the Land Down Under Multiple SQL Injection vulnerabilities.
August 31, 2005	mybbSQL.pl.txt	No	Proof of Concept exploit for the MyBB SQL Injection vulnerability.
August 31, 2005	phpldap.html phpLDAPadmin.pl.txt	No	Detailed exploitation for the phpLDAPadmin Multiple Vulnerabilities.
August 31, 2005	Xcon2005_San.pdf	N/A	Document titled, "Hacking Windows CE."
August 31, 2005	Xcon2005_SoBelt.pdf	N/A	Document titled, "Windows Kernel Pool Overflow Exploitation."
August 31, 2005	xosx-adobe-vcnative.pl xosx-adobe-vcnative-dyld.c	Yes	Exploit scripts for the Adobe Version Cue for Mac OS X Elevated Privileges vulnerabilities.
August 30, 2005	BNBTDOS.py	No	Exploit for the BNBT EasyTracker Remote Denial Of Service vulnerability.
August 24, 2005	solaris_lpd_unlink.pm.txt	Yes	This Metasploit module uses a vulnerability in the Solaris line printer daemon to delete arbitrary files on an affected system.

[back to top]

Trends

- US-CERT has received reports of multiple phishing sites that attempt to trick users into donating funds to fraudulent foundations in the aftermath of Hurricane Katrina. US-CERT warns users to expect an increase in targeted phishing emails due to recent events in the Gulf Coast Region. Source: http://www.us-cert.gov/current/.
- **The Common Malware Enumeration (CME) initiative:** Article published in the September 2005 issue of the Virus Bulletin. The Common Malware Enumeration (CME) initiative is an effort headed by the United States Computer Emergency Readiness Team (US-CERT). The CME initiative works with private industry and government to: Assign unique identifiers to high priority malware events; Facilitate the coordination of malware information; and Improve the current state of public information needed to respond to malware events. For more information about CME, see: http://cve.mitre.org/cme/.
- **New Security Technology Won't Foil Identity Theft, Researcher Warns:** According to a British criminology research new security technology such as smart ID cards or biometric safeguards won't stop identity thieves. Source: http://www.governmententerprise.com/news/showArticle.jhtml;jsessionid=3F1ACA4TVPMDAQSNDBESKHA?articleId=170700832.

- **The Four Most Common Security Dangers:** The four biggest threats are social engineering, faulty procedures, technical abuse and insider trading. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=170700829&tid=6004.
- **Arabic Trojan butts into porn surfing:** A malicious Trojan horse, Yusufali-A, that tries to interrupt the surfing of adult websites is circulating by displaying messages from the Koran. It monitors users' surfing habits by examining the title bar of the active window. Source: http://www.vnunet.com/vnunet/news/2141861/arabic-trojan-butts-porn.
- **6 ways to survive major Internet attacks:** Federal Computer Week's editors met with information technology security officials from the government and industry to discuss what is being done to help their agencies and customers secure their networks. Six ways were suggested to avoid disruptive network attacks; define the problem; consolidate standards and purchasing power; think risks; fix configurations; better people mean more secure networks; and identify problems early and react fast, Source: http://www.fcw.com/article90656-09-05-05-Print .
- **Mytob dominates August virus charts:** According to security vendors, Mytob variants accounted for over half of the virus infections found in August. Source: http://www.vnunet.com/vnunet/news/2141780/mytob-dominates-august-virus.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Zafi-D	Win32 Worm	Slight Increase	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
3	Lovgate.w	Win32 Worm	Increase	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
4	Zafi-B	Win32 Worm	Increase	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
5	Netsky-Q	Win32 Worm	Slight Decrease	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
6	Mytob.C	Win32 Worm	Decrease	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
7	Mytob-AS	Win32 Worm	Slight Decrease	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
8	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
9	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
10	Mytob-BE	Win32 Worm	Decrease	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.

Table Updated September 4, 2005

[back to top]

Last updated September 08, 2005